the enamel, flat and smooth to the stumps, exposing there a central tract of osteodentine without any sign of decay.

The paper is illustrated by a view and plans of the cavern, and by figures of the principal human remains, and of two implements of bone on which the Vicomte de Lastic had discovered, on removal of the breccia, outline figures of the head of a reindeer and the head of a horse in profile.

The description of the various remains of the animals killed for food, and of the flint- and bone-implements applied to that and other purposes, will be the subject of a future communication.

June 16, 1864.

Major-General SABINE, President, in the Chair.

Dr. Brinton; Professor Boole; Mr. T. Grubb; Sir Charles Locock, Bart.; and Mr. Nicholas Wood, were admitted into the Society.

The following communications were read:—

I. "On Complex Binary Quadratic Forms." By H. J. Stephen Smith, M.A., F.R.S., Savilian Professor of Geometry in the University of Oxford. Received May 18, 1864.

The purpose of this note is to extend to complex quadratic forms some important investigations of Gauss relating to real quadratic forms. We shall consider in order (I.) the definition of the Genera, (II.) the theory of Composition, (III.) the determination of the number of Ambiguous Classes, (IV.) the representation of forms of the principal genus by ternary quadratic forms of determinant 1. For the comparison of the numbers of classes of different orders, we may refer to a paper by M. Lipschitz (Crelle's Journal, vol. liv. p. 193); and for the principles of the theory of complex numbers and complex quadratic forms, to Lejeune Dirichlet's Memoir, "Recherches sur les formes quadratiques à coefficients et à indéterminées complexes" (Crelle, vol. xxiv. p. 291).

I. *The Definition of the Genera.*

Let $f=(a, b, c)$ be an uneven* primitive form of determinant D, and $m=ax^2+2bxy+cy^2$, $m'=ax'^2+2bx'y'+cy'^2$ two numbers represented by f. The generic characters of f are deducible from the equation

$$(ax^2+2bxy+cy^2)\ (ax'^2+2bx'y'+cy'^2)=$$
$$(axx'+b[xy'+x'y]+cyy')^2-\mathrm{D}(xy'-x'y)^2,$$

* A primitive form (a, b, c) is uneven, semieven, or even, according as the greatest common divisor of a, $2b$, c is 1, $1+i$, or $(1+i)^2$; *i.e.*, in Lejeune Dirichlet's nomenclature, according as (a, b, c) is of the first, second, or third species. In this paper, when we speak of an uneven, semieven, or even form or class, we shall always suppose the form or class to be primitive. A semieven number is a number divisible by $1+i$, but not by $(1+i)^2$.

or, as we shall write it,

$$mm' = P^2 - DQ^2.$$

Thus, supposing that p is an uneven prime dividing D, and that m and m' are prime to p, the numbers prime to p, which are represented by f, are either all quadratic residues of p, or else all non-quadratic residues of p; in the former case we attribute to f the character $\left[\frac{f}{p}\right] = +1$, in the latter the character $\left[\frac{f}{p}\right] = -1$.

Again, to investigate the supplementary characters relating to powers of the even prime $1+i$, let $m = \mu + i\mu'$ be an uneven number, μ and μ' representing real numbers, and for brevity, let

$$(-1)^{\frac{1}{4}(N.m-1)} = \alpha,$$
$$(-1)^{\frac{1}{8}[(\mu+\gamma\mu')^2-1]} = \beta,$$
$$(-1)^{\mu'} = \gamma.$$

The values of the units, or *characters*, α, β, γ depend on the residue of m for the modulus $(1+i)^5$, as is shown in the following Table.

TABLE I.

$m \equiv$	$\alpha =$	$\beta =$	$\gamma =$
± 1	$+1$	$+1$	$+1$
$\pm i$	$+1$	$+1$	-1
± 3	$+1$	-1	$+1$
$\pm 3i$	$+1$	-1	-1
$\pm(1-2i)$ ..	-1	$+1$	$+1$
$\pm(2+i)$	-1	$+1$	-1
$\pm(1+2i)$ ..	-1	-1	$+1$
$\pm(2-i)$	-1	-1	-1

An inspection of the Table shows that, of the sixteen uneven residues of $(1+i)^5$, eight have the character $\omega = 1$, and eight the character $\omega = -1$, ω representing any one of the seven characters α, β, γ, $\beta\gamma$, $\alpha\gamma$, $\alpha\beta$, $\alpha\beta\gamma$. It will also be seen that any character of a product of two uneven factors

is found by multiplying together the corresponding characters of the factors; so that, conversely, according as any character of a product of two uneven factors is $+1$ or -1, the two factors agree or differ in respect of that character.

The next Table assigns the supplementary characters proper to any given determinant; they depend on the residue of the determinant for the modulus $(1+i)^5$.

TABLE II.

D $\equiv$	Characters.	D $\equiv$	Characters.
$\pm(1+i)$....	β	± 1	γ
$\pm(1-i)$....	$\alpha\beta$	$\pm i$	α
$\pm(3+i)$....	$\alpha\beta\gamma$	± 3	γ
$\pm(3-i)$....	$\beta\gamma$	$\pm 3i$	α
± 2.....	α, γ	$\pm(1-2i)$	γ
$\pm 2i$	γ	$\pm(2+i)$	$\alpha\gamma$
$2(1+i)$	$\alpha\beta, \gamma$	$\pm(1+2i)$	γ
$2(1-i)$	β, γ	$\pm(2-i)$	$\alpha\gamma$
4.....	α, γ		
0.....	α, β, γ		

Of the eighteen propositions contained in this Table, it will suffice to enunciate and demonstrate one.

"If D $\equiv \pm(3+i)$, mod $(1+i)^5$, and f is an uneven form of determinant D, the uneven numbers represented by f, all have the character $\alpha\beta\gamma=+1$, or else all have the character $\alpha\beta\gamma=-1$."

In the equation $P^2-DQ^2=mm'$, let us suppose that m and m' are uneven; then P is uneven because D is semieven; also $Q^2 \equiv \pm 1, \pm 2i$, 4 or 0, mod $(1+i)^5$, according as the index of the highest power of $1+i$ dividing Q is 0, 1, 2, or >2. If Q is uneven, $mm' \equiv \pm 3i$ or $\pm(2+i)$, mod $(1+i)^5$; if Q is semieven, $mm' \equiv \pm(1+2i)$, mod $(1+i)^5$; if Q is even, $mm' \equiv \pm 1$, mod $(1+i)^5$; *i. e.* in all three cases mm' has the character $\alpha\beta\gamma=1$, and m and m' both have the character $\alpha\beta\gamma=+1$, or else both have the character $\alpha\beta\gamma=-1$.

We add a third Table for the purpose of distinguishing between the possible and impossible genera. In this Table S^2 is the greatest square dividing D, P is uneven and primary*, I is the index of the highest power of $1+i$ dividing S, ϖ represents an uneven prime dividing P, σ an uneven prime dividing S but not P. For brevity, the symbols ϖ and σ are written instead of $\left[\frac{f}{\varpi}\right]$ and $\left[\frac{f}{\sigma}\right]$.

* By a primary uneven number we understand (with Lejeune Dirichlet) an uneven number $\mu+\mu' i$ satisfying the congruences $\mu \equiv 1$, mod 4, $\mu' \equiv 0$, mod 2.

TABLE III.

(i) $D=PS^2$, $P\equiv 1$, mod 4.

I=0, 1	ϖ	σ, γ
I=2	ϖ	σ, γ, α
I>2	ϖ	$\sigma, \gamma, \alpha, \beta.$

(ii) $D=PS^2$, $P\equiv 1+2i$, mod 4.

I=0, 1	ϖ, γ	σ
I=2	ϖ, γ	σ, α
I>2	ϖ, γ	$\sigma, \alpha, \beta.$

(iii) $D=iPS^2$, $P\equiv 1$, mod 4.

I=0	ϖ, α	σ
I=1, 2	ϖ, α	σ, γ
I>2	ϖ, α	$\sigma, \gamma, \beta.$

(iv) $D=iPS^2$, $P\equiv 1+2i$, mod 4.

I=0	$\varpi, \alpha\gamma$	σ
I=1, 2	ϖ, α, γ	σ
I>2	ϖ, α, γ	$\sigma, \beta.$

(v) $D=(1+i)PS^2$, $P\equiv 1$, mod 4.

I=0	ϖ, β	σ
I=1	ϖ, β	σ, γ
I>1	ϖ, β	$\sigma, \gamma, \alpha.$

(vi) $D=(1+i)PS^2$, $P\equiv 1+2i$, mod 4.

I=0	$\varpi, \beta\gamma$	σ
I=1	ϖ, β, γ	σ
I>1	ϖ, β, γ	$\sigma, \alpha.$

(vii) $D=i(1+i)PS^2$, $P\equiv 1$, mod 4.

I=0	$\varpi, \alpha\beta$	σ
I=1	$\varpi, \alpha\beta$	σ, γ
I>1	ϖ, α, β	$\sigma, \gamma.$

(viii) $D=i(1+i)PS^2$, $P\equiv 1+2i$, mod 4.

I=0	$\varpi, \alpha\beta\gamma$	σ
I=1	$\varpi, \alpha\beta, \gamma$	σ
I>1	$\varpi, \alpha, \beta, \gamma$	$\sigma.$

The characters preceding the vertical line by which the Table is divided are not independent, but are subject to the condition (arising from the laws of quadratic residues) that their product must be a positive unit. To show that this is so, let $D=i^{\alpha'}(1+i)^{\beta'}PS^2$, where α' and β' are each either 0 or 1; also let $\gamma'=0$, or 1, according as $P\equiv 1$, or $\equiv 1+2i$, mod 4. If m is a number prime to $(1+i)D$ and capable of primitive representation*

* If $m=ax^2+2bxy+cy^2$, the representation of m by (a, b, c) is said to be primitive when the values of the indeterminates are relatively prime.

by f, the congruence $\omega^2 \equiv D$, mod m, is resoluble; and its resolubility implies the condition $\left[\frac{D}{m}\right] = \left[\frac{i^{\alpha'}}{m}\right] \times \left[\frac{(1+i)^{\beta'}}{m}\right] \times \left[\frac{P}{m}\right] = 1$. But, by the laws of quadratic residues, $\left[\frac{i}{m}\right] = \alpha$, $\left[\frac{1+i}{m}\right] = \beta$, $\left[\frac{P}{m}\right] = \gamma^{\gamma'}\left[\frac{m}{P}\right]$; and the condition just written becomes $\alpha^{\alpha'}\beta^{\beta'}\gamma^{\gamma'}\left[\frac{m}{P}\right] = 1$, which is coincident with that indicated in the Table. Thus (as in the real theory) one-half of the whole number of assignable generic characters are impossible*; we shall presently obtain a different proof of this result, and shall also show that the remaining half correspond to actually existing genera.

For the characters of a semieven form f, it is convenient to take the characters of the numbers represented by $\frac{f}{1+i}$; and for the characters of an even form, the characters of the numbers represented by $\frac{f}{2i}$. The following Table will serve to form the complete generic character in each case.

For a semieven form.

(i) $D \equiv PS^2$, $P \equiv 1$, mod 4.

$$I = 0 \mid \varpi \mid \sigma.$$

(ii) $D \equiv PS^2$, $P \equiv 1 + 2i$, mod 4.

$$I = 0 \mid \varpi, \gamma \mid \sigma.$$

For an even form.

$$I = 0 \mid \varpi \mid \sigma.$$

II. *The Theory of Composition.*

The theory of composition given in the 'Disquisitiones Arithmeticæ' is immediately applicable to complex quadratic forms. There are, however, a few points to which we must direct attention.

(1) If m_1, m_2, m_3 are the greatest common divisors of $a, 2b, c$; $a, (1+i)b, c$; a, b, c, we have

(i) $m_1 = m_2 = m_3$,

(ii) $m_1 = m_2 = (1+i)m_3$,

(iii) $m_1 = (1+i)m_2 = (1+i)^2 m_3$,

according as (a, b, c) either is, or is derived from, (i) an uneven, (ii) a semieven, (iii) an even primitive. Hence the order of a form is given when m_1 and m_3 are given. Thus, if F is compounded of f and f', and if $M_1 M_2 M_3$, $m_1 m_2 m_3$, $m'_1 m'_2 m'_3$ refer to F, f, f' respectively, the order of F is completely determined by the two theorems, "M_1 is the product of m_1 and

* The determinant is supposed not to be a square.

m_1'." "$\frac{M_1}{M_3}$ is the least common multiple of $\frac{m_1}{m_3}$ and $\frac{m'_1}{m'_3}$." (Gauss's 5th and 6th conclusions, Disq. Arith. art. 235.)

It will be found that Gauss's proof of these theorems can be transferred to the complex theory; only, when f and f' are both semieven, or derived from semieven primitives, the proof of the sixth conclusion is incomplete, and, while showing that F cannot be derived from an uneven primitive, fails to show whether it is derived from a semieven or from an even primitive. But, in the same way in which Gauss has shown that M_1 is divisible by $m_1 \times m'_1$, it can also be shown that M_2 is divisible by $m_2 \times m'_2$*; *i. e.*, in the case which we are considering, M_2 is divisible by M_1, because $m_2 = m_1$, $m'_2 = m'_1$, and $m_1 m'_1 = M_1$. Therefore $M_2 = M_1$, and F is derived from a semieven primitive in accordance with our enunciation of Gauss's sixth conclusion.

(2) In the real theory, when two or more forms are compounded, each form may be taken either directly or inversely; but, however the forms are taken, the determinant of the resulting form is the same. In the complex theory, not only may each of the forms to be compounded be taken in either of two different ways, but also the determinant of the resulting form may receive either of two values, differing, however, only in sign; and it is important to attend to the ambiguities which thus arise. If a complex rational number n be written in the form $i^\lambda(1+i)^\mu \frac{P}{Q}$, where λ is 0, 1, 2, or 3, μ is any positive or negative integer, and P, Q are primary uneven complex integers, we may term i^λ the sign of n. Let F, of which the determinant is D, be transformed into the product $f_1 \times f_2 \times \ldots f_h$, by a substitution [X, Y] linear and homogeneous in respect of h binary sets; we have, as in the real theory, h equations of the type

$$\left(\frac{dX}{dx_k}\frac{dY}{dy_k} - \frac{dX}{dy_k}\frac{dY}{dx}\right)^2 = \frac{d_k}{D} \times \frac{\Pi \cdot f^2}{f^2_k},$$

d_k representing the determinant of f_k. Let

$$n_k = \left(\frac{dX}{dx_k}\frac{dY}{dy_k} - \frac{dX}{dy_k}\frac{dY}{dx_k}\right) \div \frac{\Pi \cdot f}{f_k},$$

so that $n^2_k = \frac{d_k}{D}$; if i^{λ_k} is the sign of n_k, we shall say that f_k is taken with the sign i^{λ_k}. We can thus enunciate the theorem, "Forms, compounded of the same forms, taken with the same signs, are equivalent." If f_1, $f_2 \ldots f_h$ are given forms which it is required to compound, the signs of $d_1, d_2, \ldots d_h$ must be all real, or else all unreal; and the sign of D will be real or unreal accordingly. The value of D (irrespective of its sign) is ascertained as in the real theory; but it may receive at our option, in the

* Disq. Arith. art. 235. The proof that $2(bb'+\Delta)$ and $2(bb'-\Delta)$ are divisible by $m_1 \times m'_1$, may be employed (*mutatis mutandis*) to show that $(1+i)(bb'+\Delta)$ and $(1+i)(bb'-\Delta)$ are divisible by $m_2 \times m'_2$.

one case, either of the two real signs, and in the other case either of the two unreal signs. And whichever sign we give to D, the form f_k may be taken with either of the two real signs, if the sign of $\frac{d^k}{D}$ is $+1$, and with either of the two unreal signs, if the sign of $\frac{d_k}{D}$ is -1. In the important case in which $d_1, d_2 \ldots$ all have the same sign, we shall always suppose D to have that sign, and $f_1, f_2 \ldots$ to be all taken with the sign $+1$. Adopting this convention, we see that the class compounded of given classes of the same determinant, or of different determinants having the same sign, is defined without ambiguity.

(3) By the general formulæ of M. Arndt (Crelle, vol. lvi. p. 69), which on account of their great utility we transcribe here, we can always obtain a form (A, B, C) compounded in any given manner of two forms (a, b, c) and (a', b', c'), of which the determinants d and d' are to one another as two squares.

$$\left.\begin{aligned} A &= \frac{aa'}{\mu^2} \\ \frac{an'}{\mu} B &\equiv \frac{ab'}{\mu} \\ \frac{a'n}{\mu} B &\equiv \frac{a'b}{\mu} \\ \frac{bn'+b'n}{\mu} B &\equiv \frac{bb'+Dnn'}{\mu} \end{aligned}\right] \text{mod } A$$

$$C = \frac{B^2 - D}{A}.$$

In these formulæ D is the greatest common divisor of dm'^2 and $d'm^2$, m and m' representing the greatest common divisors of a, $2b$, c, and a', $2b'$ c'; n and n' are the square roots of $\frac{d}{D}$ and $\frac{d'}{D}$; μ is the greatest common divisor of an', $a'n$, and $bn'+b'n$. The signs of D, n, and n' are given, because the manner of the composition is supposed to be given; to μ we may attribute any sign we please, because the forms (A, B, C) and $(-A, B, -C)$ are equivalent.

(4) If F= (A, B, C) is compounded of two primitive forms f and f', and if M is the highest power of $1+i$ dividing A, B, C (so that M is 1, or $1+i$, or $(1+i)^2$), the complete character of the primitive form $\frac{1}{M}$ F is obtained by the following rule:—

"If ω is any character common to f and f', $\frac{1}{M}$ F will have the character $\omega = +1$, or $\omega = -1$, according as f and f' agree or differ in respect of that character."

In comparing the characters of f and f', it is to be observed that if ω and ω' are two supplementary characters of f, and $\omega \times \omega'$ a supplementary character of f', $\omega \times \omega'$ is to be regarded as a character common to f and f'.

(5) Let us represent by (1), (σ), and (Σ)* respectively the principal uneven, semieven, and even classes of determinant D; *i. e.* the classes containing the forms $(1, 0, -D)$, $\left(1+i, 1, -\frac{D-1}{1+i}\right)$, and $\left(2i, i^k, -\frac{D-i^{2k}}{2i}\right)$, the existence of the last two classes implying the congruences $D\equiv 1$, mod 2, $D\equiv i^{2k}$, mod 4, respectively. Employing the formulæ of M. Arndt, we find $(f)\times(1)=(f)$, if (f) is any class of determinant D; $(f)\times(\sigma)=(1+i)(f)$, if f is derived from a semieven or even primitive; $(f)\times(\Sigma)=2i(f)$, if f is derived from an even primitive; and, in particular, $(1)\times(1)=(1)$, $(\sigma)\times(\sigma)=(1+i)(\sigma)$, $(\Sigma)\times(\Sigma)=2i(\Sigma)$. Also, if (f) and (f^{-1}) are two opposite primitive classes, $(f)\times(f)^{-1}=(1)$, or $(1+i)(\sigma)$, or $2i(\Sigma)$, according as f and f^{-1} are uneven, semieven, or even. Hence the three equations $(f_1)\times(\phi)=(f_2)$, $(f_1)\times(\phi)=(1+i)(f_2)$, $(f_1)\times(\phi)=2i(f_2)$, in which (f_1) and (f_2) are given primitive classes, uneven in the first, semieven in the second, and even in the third, are respectively satisfied by the uneven, semieven, and even classes $(\phi)=(f_2)\times(f_1)^{-1}$, $(\phi)=\frac{(f_2)\times(f_1)^{-1}}{1+i}$, $(\phi)=\frac{(f_2)\times(f_1)^{-1}}{2i}$, but by no other classes whatever. Again, let $D=\Delta m^2$ and let the forms (mp, mq, mr), $([1+i]mp, mq, [1+i]mr)$, $(2imp, mq, 2imr)$ represent classes derived by the multiplier m from uneven, semieven, and even primitives of determinant Δ; in all three forms we suppose p prime to 2D; in the second and third we suppose q uneven, and $\Delta\equiv 1$, mod 2; in the third we suppose $\Delta\equiv i^{2k}$, mod 4. The formulæ of M. Arndt will then establish the six equations,—

$$(m, 0, -\Delta m)\times(p, mq, m^2r)=(mp, mq, mr),$$

$$\left([1+i]m, m, -m\frac{\Delta-1}{1+i}\right)\times(p, mq, 2im^2r)=([1+i]mp, mq, [1+i]mr),$$

$$\left(2im, i^km, -m\frac{\Delta-i^{2k}}{2i}\right)\times(p, mq, -4m^2r)=(2imp, mq, 2imr),$$

$$\left([1+i]m, m, -m\frac{\Delta-1}{1+i}\right)\times([1+i]p, mq, [1+i]m^2r)$$
$$=(1+i)\times([1+i]mp, mq, [1+i]mr),$$

$$\left(2im, i^km, -m\frac{\Delta-i^{2k}}{2i}\right)\times([1+i]p, mq, 2i[1+i]m^2r)$$
$$=(1+i)\times(2imp, mq, 2imr),$$

$$\left(2im, i^km, -m\frac{\Delta-i^{2k}}{2i}\right)\times(2ip, mq, 2im^2r)=2i\times(2imp, mq, 2imr).$$

* It is often convenient to symbolize a class by placing within brackets a symbol representing a form contained in the class; thus (f) may be used to symbolize the class contain ng the form f.

From these equations, which contain a solution (for complex numbers) of the problem solved for real numbers in art. 250 of the 'Disquisitiones Arithmeticæ,' we may infer the following theorems (Disq. Arith. art. 251 and 253):—

"The number ω of classes of any order Ω is a divisor of the number n of uneven classes of the same determinant D; and, given any two classes of order Ω, there are always $\frac{n}{\omega}$ uneven classes which compounded with one of them produce the other."

"If $D \equiv 1$, mod 2, and if the classes of Ω are derived from semieven or even primitives, ω is a divisor of the number n' of semieven classes of determinant D; and, given any two classes of order Ω, there are always $\frac{n'}{\omega}$ semieven classes which compounded with one of them produce $1+i$ times the other."

"If $D \equiv \pm 1$, mod 4, and if the classes of Ω are derived from even primitives, ω is a divisor of the number n'' of even classes of determinant D; and, given any two classes of order Ω, there are always $\frac{n''}{\omega}$ even classes which compounded with one of them produce $2i$ times the other."

III. *Determination of the number of Ambiguous Classes.*

Any form (A, B, C), in which $2B \equiv 0$, mod A, is called by Gauss an ambiguous form; but in the investigation which follows we shall for brevity understand by an ambiguous form an uneven form of one of the four types

(i) (A, 0, C),
(ii) ([1+i] B, B, C),
(iii) (2B, B, C),
(iv) ($2i$ B, B, C).

To determine the number of uneven ambiguous classes of any determinant D supposed not to be a square, we shall determine, first, the number of ambiguous forms of determinant D; and secondly the number of ambiguous forms in each ambiguous class.

(1) Let μ be the number of different uneven primes dividing D. The number of ambiguous forms of the type (i) is $4 \times 2^{\mu}$, or $8 \times 2^{\mu}$, according as D is, or is not, uneven. For we may resolve $-D$ into any two relatively prime factors, and may take one of them (with any sign we please) for A, and the other for C. There are no ambiguous forms of the type (ii), unless $D \equiv i$, mod 2, or $\equiv 0$, mod $(1+i)^3$. For in the equation $D = B\,(B-[1+i]\,C)$, if B is uneven, we have $D \equiv i$, mod 2, because C must be uneven; if B is semieven or even, we have $D \equiv 0$, mod $(1+i)^3$. If $D \equiv i$, mod 2, we resolve D into any two relatively prime factors X and Y, and writing $B = X$, $B-(1+i)\,C = Y$, we find $C = \frac{X-Y}{1+i}$, which is in-

tegral because X and Y are uneven, and uneven because X is not $\equiv$Y, mod 2. Thus if $D \equiv i$, mod 2, there are $4 \times 2^{\mu}$ ambiguous forms of the type (ii). Again, if $D \equiv 0$, mod $(1+i)^3$, we may resolve D in any way we please into two factors having $1+i$ for their greatest common divisor; we find in this way $8 \times 2^{\mu}$ ambiguous forms of the type (ii). There are no ambiguous forms of the types (iii) or (iv), unless $D \equiv 1$, mod 2, or $\equiv 2$, mod 4, or $\equiv 0$, mod $(1+i)^5$. For if in the equation $D = B(B-2C)$, we suppose B uneven, we find $D \equiv 1$, mod 2; if B is semieven, $B^2 \equiv 2i$, and $2BC \equiv 2(1+i)$, mod 4, whence $D \equiv 2$, mod 4; lastly, if B is even, $D \equiv 0$, mod $(1+i)^5$. The same reasoning applies to the equation $D = B(B-2iC)$. If $D \equiv 1$, mod 2, we resolve D in every possible way into the product of two factors relatively prime; let $D = X \times Y$ be such a resolution, then $D = iX \times -iY$ is another; and it will be seen that according as the last coefficient in the two forms

$$\left[2X, X, \frac{X-Y}{2}\right], \quad \left[2iX, X, \frac{X-Y}{2i}\right]$$

is uneven or not uneven, so the last coefficient in the two forms

$$\left[2iX, iX, \frac{iX+iY}{2}\right], \quad \left[-2X, iX, \frac{X+Y}{2}\right],$$

is not, or is, uneven; *i. e.* there are $2 \times 2^{\mu}$ ambiguous forms of each of the types (iii) and (iv). If $D \equiv 2$, mod 4, we resolve D in every possible way into two factors, of which $1+i$ is the greatest common divisor; we thus find $4 \times 2_{\mu}$ uneven forms of each of the types (iii) and (iv). Lastly, if $D \equiv 0$, mod $(1+i)^5$, we resolve D in every possible way into two factors of which $1+i$ is the greatest common divisor, and we obtain 8×2 forms of each of the types (iii) and (iv).

The result of this enumeration is that if D be uneven, or semieven, or $\equiv 2i$, mod 4, there are $8 \times 2^{\mu}$ ambiguous forms; if $D \equiv 2$, mod 4, or $\equiv 0$, mod $(1+i)^3$, but not mod $(1+i)^5$, there are $16 \times 2^{\mu}$; and if $D \equiv 0$, mod $(1+i)^5$, there are $32 \times 2^{\mu}$. On comparing this result with Table III., it will be seen that in every case there are four times as many ambiguous forms as there are assignable generic characters.

(2) Let $f = (a, b, c)$ be any form of an ambiguous class; if $(I) = \begin{vmatrix} \mu, & -\lambda \\ \nu, & -\mu \end{vmatrix}$ is an improper automorphic of f, λ, μ, ν satisfy the equations

$$\mu^2 - \lambda\nu = 1, \quad \ldots\ldots\ldots\ldots \quad (1)$$

$$\lambda a + 2\mu b + \nu c = 0; \quad \ldots\ldots\ldots\ldots \quad (2)$$

and, conversely, if λ, μ, ν satisfy the equations (1) and (2), $(I) = \begin{vmatrix} \mu, & -\lambda \\ \nu, & -\mu \end{vmatrix}$ is an improper automorphic of f. Let α, γ, p, q (of which α and γ are relatively prime) be a system of integral numbers satisfying the equations

$$\left.\begin{aligned} p\alpha &= \lambda, & p\gamma &= \mu - 1, \\ q\alpha &= \mu + 1, & q\gamma &= \nu; \end{aligned}\right\} \quad \ldots\ldots\ldots \quad (3)$$

and let $\theta=0$, $1-i$, 1, or $-i$, according as 0, $1-i$, 1 or $-i$ satisfies the congruences

$$p+\theta\alpha\equiv 0, \text{ mod } 2,$$
$$q+\theta\gamma\equiv 0, \text{ mod } 2,$$

which are simultaneously resoluble, and admit of only one solution, because α and γ are relatively prime, while $q\alpha-p\gamma=2$. Then it will be found that by the proper transformation

$$(\mathrm{J})=\begin{vmatrix}\alpha, & \frac{1}{2}(p+\theta\alpha)\\ \gamma, & \frac{1}{2}(q+\theta\gamma)\end{vmatrix}$$

f is transformed into an ambiguous form ϕ, which will be of the type (i), (ii), (iii), or (iv), according as $\theta=0$, $1-i$, 1, or $-i$. It will also be seen that, subject to the condition that α and γ are relatively prime, there are always four, and only four, solutions of the system (3), represented by the formula

$$i^k\alpha, \quad i^k\gamma, \quad i^{-k}p, \quad i^{-k}q.$$

There are thus four transformations included in the formula (J), two of them transforming f into the same ambiguous form ϕ, and the other two transforming f into the same form taken negatively. The four transformations (J), and the two ambiguous forms ϕ and $-\phi$, we shall term respectively the transformations and the ambiguous forms appertaining to the improper automorphic (I). If we now form the transformations appertaining to every improper automorphic of f, it can be proved (A) that these transformations will all be different, and (B) that they will include every proper transformation of f into an ambiguous form.

(A) As the four transformations appertaining to the same improper automorphic are evidently different, it will be sufficient to show that if (J) and (J′) appertain to the improper automorphics (I) and (I′), the supposition (J)=(J′) implies (I)=(I′). From the equations

$$\alpha=\alpha', \quad \gamma=\gamma', \quad p+\theta\alpha=p'+\theta'\alpha', \quad q+\theta\gamma=q'+\theta'\gamma'$$

(which are equivalent to the symbolic equation (J)=(J′)), combined with the system (3), and with a similar system containing the accented letters, we find

$$(\theta-\theta')\alpha^2=\lambda'-\lambda,\ (\theta-\theta')\alpha\gamma=\mu'-\mu,\ (\theta-\theta')\gamma^2=\nu-\nu';$$

whence again $(\theta-\theta')(a\alpha^2+2b\alpha\gamma+c\gamma^2)=0$, by virtue of equation (2). The coefficient of $\theta-\theta'$ is not zero, for $\mathrm{D}=b^2-ac$ is not a square; therefore $\theta-\theta'=0$; *i. e.* $\lambda=\lambda'$, $\mu=\mu'$, $\nu=\nu'$, or (I)=(I′).

(B) Let $\begin{vmatrix}\alpha, & \beta\\ \gamma, & \delta\end{vmatrix}$ be a proper transformation of f into an ambiguous form ϕ; according as ϕ is of the type (i), (ii), (iii), or (iv), let $\theta=0$, $1-i$, 1, or $-i$; let also $\lambda=2\alpha\beta-\theta\alpha^2$, $\mu=\alpha\delta+\beta\gamma-\theta\alpha\gamma$, $\nu=2\gamma\delta-\theta\gamma^2$; then $\begin{vmatrix}\mu, & -\lambda\\ \nu, & -\mu\end{vmatrix}$ =(I) is an improper automorphic of f; for

$$\mu^2-\lambda\nu=(\alpha\delta-\beta\gamma)^2=1, \quad \text{and } \lambda a+2\mu b+\nu c=0,$$

because of the ambiguity of the form into which f is transformed by

$\left|\begin{matrix}\alpha, & \beta\\ \gamma, & \delta\end{matrix}\right|$. Also $\left|\begin{matrix}\alpha, & \beta\\ \gamma, & \delta\end{matrix}\right|$ appertains to (I); for, writing p and q instead of $2\beta-\theta\alpha$, and $2\delta-\theta\gamma$, we have $\left|\begin{matrix}\alpha, & \beta\\ \gamma, & \delta\end{matrix}\right| = \left|\begin{matrix}\alpha, & \frac{1}{2}(p+\theta\alpha)\\ \gamma, & \frac{1}{2}(q+\theta\gamma)\end{matrix}\right|$, α, γ, p, q (of which α and γ are relatively prime) being four numbers which satisfy the system (3); *i. e.* $\left|\begin{matrix}\alpha, & \beta\\ \gamma, & \delta\end{matrix}\right|$ appertains to (I), an improper automorphic of f.

It follows from (B) that, if we calculate the ambiguous forms ϕ and $-\phi$ appertaining to every improper automorphic of f, we shall obtain all the ambiguous forms to which f is equivalent; it remains to see how many of these ambiguous forms are different from one another. If (I) $= \left|\begin{matrix}\mu, & -\lambda\\ \nu, & -\mu\end{matrix}\right|$ is any given improper automorphic of f, all its similar automorphics are contained in the four formulæ

$$(\mathrm{T})^{2k}\times(\mathrm{I}),\ (\mathrm{T})^{2k+1}\times(\mathrm{I}),\ (\mathrm{T})^{2k}\times\left|\begin{matrix}-1, & 0\\ 0, & -1\end{matrix}\right|\times(\mathrm{I}),$$

$$(\mathrm{T})^{2k+1}\times\left|\begin{matrix}-1, & 0\\ 0, & -1\end{matrix}\right|\times(\mathrm{I}),$$

where k is any positive or negative number, and $(\mathrm{T}) = \left|\begin{matrix}t_1-u_1 b, & -u_1 c\\ u_1 a, & t_1+u_1 b\end{matrix}\right|$, $[t_1, u_1]$ representing a fundamental solution of the equation $t^2-\mathrm{D}u^2=1$. Similarly, if (J) represent the four transformations, appertaining to (I), by which f passes into ϕ or $-\phi$, all the proper transformations of f into ϕ or $-\phi$ are included in the formula $(\mathrm{T})^k\times(\mathrm{J})$. We shall now show that the four transformations included in the formula $(\mathrm{T})^k\times(\mathrm{J})$ appertain to the improper automorphic $(\mathrm{T})^{2k}\times(\mathrm{I})$. Writing

$$\alpha_k=(t_k-bu_k)\alpha-cu_k\gamma, \qquad p_k=(t_k-bu_k)p-cu_kq,$$
$$\gamma_k=au_k\alpha+(t_k+bu_k)\gamma, \qquad q_k=au_kp+(t_k+bu_k)q,$$
$$\lambda_{2k}=(t_{2k}-bu_{2k})\lambda-cu_{2k}\mu,$$
$$\mu_{2k}=(t_{2k}-bu_{2k})\mu-cu_{2k}\nu=au_{2k}\lambda+(t_{2k}+bu_{2k})\mu,$$
$$\nu_{2k}=au_{2k}\mu+(t_{2k}+bu_{2k})\nu,$$

we find immediately

$$(\mathrm{T})^k\times(\mathrm{J})=\left|\begin{matrix}\alpha_k, & \frac{1}{2}(p_k+\theta\alpha_k)\\ \gamma k, & \frac{1}{2}(q_k+\theta\gamma_k)\end{matrix}\right|,\quad (\mathrm{T})^{2k}\times(\mathrm{I})=\left|\begin{matrix}\mu_{2k}, & -\lambda_{2k}\\ \nu_{2k}, & -\mu_{2k}\end{matrix}\right|.$$

Also attending to the equations (2) and (3), and to the relations

$$t_{2k}=t^2{}_k-\mathrm{D}u^2{}_k,\quad u_{2k}=2t_k u_k,$$

we obtain, after substitution and reduction,

$$p_k\alpha_k=\lambda_{2k}, \qquad p_k\gamma_{2k}=\mu_{2k}-1,$$
$$q_k\alpha_k=\mu_{2k}+1, \quad q_k\gamma_k=\nu_{2k},$$

i. e. $(\mathrm{T})^k\times(\mathrm{J})$ appertains to $(\mathrm{T})^{2k}\times(\mathrm{I})$, if (J) appertains to (I).

It follows from this result that the ambiguous forms appertaining to (I) and to (T) $\times$ (I) are the same; for f is transformed into the same forms by (J) and (T) $\times$ (J); and conversely, if the ambiguous forms appertain-

ing to two different automorphics (I) and (I′) are identical, an equation of the form $(I')=T^{2k}\times(I)$ will subsist; for if (J) and (J′) are the transformations appertaining to (I) and (I′), since by hypothesis (J) and (J′) transform f into the same form, we must have an equation of the form $(J')=(T)^k\times(J)$; but (J′) appertains to (I′), and $(T)^k\times(J)$ to $(T)^{2k}\times(I)$; therefore $(I')=(T)^{2k}\times(I)$, by what has been shown above (A).

If then we calculate the eight ambiguous forms appertaining to the four improper automorphics

$$(I),\ \begin{pmatrix}-1, & 0\\ 0, & -1\end{pmatrix}\times(I),\ (T)\times(I),\ \begin{pmatrix}-1, & 0\\ 0, & -1\end{pmatrix}\times(T)\times(I),$$

these eight forms will be the only ambiguous forms equivalent to f. Thus every uneven ambiguous class contains eight ambiguous forms.

Combining this result with the preceding we obtain the Theorem,

"The number of uneven ambiguous classes is one half of the whole number of assignable generic characters."

The number of semieven and even ambiguous classes is determined by the two following Theorems:—

"When $D\equiv\pm1$, mod 4, there are as many even as semieven ambiguous classes."

"When $D\equiv1$, mod 2, there are as many semieven as uneven ambiguous classes, or only half as many, according as there are altogether as many semieven as uneven classes, or only half as many."

To prove the first of these theorems, let $D\equiv i^{2k}$, mod 4, and let

$$\Sigma=\left(2i,\ i^k,\ \frac{i^{2k}-D}{2i}\right);$$

it is evident from the principles of the composition of forms that if (ϕ) is a given semieven ambiguous class, the equation $(\Sigma)\times(\phi)=(1+i)\times(f)$ is satisfied by one and only one even ambiguous class (f); in addition to this we shall now show that, if (f) is a given even ambiguous class, the same equation is satisfied by one and only one semieven ambiguous class (ϕ); from which two things the truth of the theorem is manifest. First, let the whole number of even classes be equal to the whole number of semieven classes*; then the equation

$$(\Sigma)\times(\phi)=(1+i)\times(f)$$

* That if $D\equiv\pm1$, mod 4, there are either as many semieven as even classes, or else three times as many, is a theorem of M. Lipschitz (Crelle, vol. liv. p. 196), of which it is worth while to give a proof here. The number of even classes is to the number of semieven classes, as unity to the number of semieven classes satisfying the equation

$$(\Sigma)\times(\phi)=(1+i)\times(f),$$

f representing any given even form. To investigate the semieven classes satisfying this equation, apply to f a complete system of transformations for the modulus $1+i$, for example, the transformations

$$\begin{vmatrix}1, & 0\\ 0, & 1+i\end{vmatrix},\quad \begin{vmatrix}1+i, & 0\\ 0 & 1\end{vmatrix},\quad \begin{vmatrix}1+i, & 1\\ 0, & 1\end{vmatrix},$$

is satisfied by only one semieven class (ϕ); and this class is ambiguous, for the equation is satisfied by the opposite of (ϕ) as well as by (ϕ) itself; therefore (ϕ) and its opposite are the same class, or (ϕ) is an ambiguous class. Secondly, let the number of semieven classes be three times the number of even classes; then the equation

$$(\Sigma)\times(\phi)=(1+i)\,(f)$$

is satisfied by three and only three different classes (ϕ); but it is also satisfied by the opposites of these classes; therefore one of them is necessarily an ambiguous class. Let that class be (ϕ_0); the other two are defined by the equations

$$(1+i)\,(\phi_1)=(\sigma_1)\times(\phi_0),\quad (1+i)\,(\phi_2)=(\sigma_2)\times(\phi_0),$$

and cannot be ambiguous classes; for by duplication we find

$$(\phi_1)\times(\phi_1)=(1+i)\,(\sigma_2),\quad (\phi_2)\times(\phi_2)=(1+i)\,(\sigma_1);$$

whereas every semieven ambiguous class produces $(1+i)\sigma_0$ by its duplication *.

The second theorem may be proved as follows. Let

$$f=([1+i]p,\ q,\ [1+i]r)$$

be a semieven form of determinant D; and let

$$\sigma_0=\left((1+i),\ 1,\ -\frac{D-1}{1+i}\right);$$

we suppose that p is uneven. The equation $(\sigma_0)\times(\phi)=(f)$ is satisfied by one uneven class (ϕ_0), or by two (ϕ_0) and (ϕ_1), according as the forms $\phi_0=(p,\ q,\ 2ir)$, and $\phi_1=(2ip,\ q,\ r)$, if r is uneven, or the forms $\phi_0=(p,\ q,\ 2ir)$, and $\phi_1=(2ip,\ [1+i]p+q,\ p+[1-i]q+r)$, if r is even, are or are not equivalent†. If any one of the forms f, ϕ_0, ϕ_1 is ambiguous, the others are so too; the same thing is therefore true for the classes (f), (ϕ_0), (ϕ_1). Thus the number of semieven ambiguous classes is equal to or

---

and divide the resulting forms by $1+i$; of the quotients, one, or three, will be semieven, according as $D\equiv\pm1$, or ±5, mod $(1+i)^5$. It will be found that each of these semieven forms satisfies the equation $\Sigma\times\phi=(1+i)\times f$; and, conversely, every semieven form ϕ satisfying that equation is equivalent to one of these forms; for, from any transformation of $(1+i)f$ into $\Sigma\times\phi$, we may (by attributing to the indeterminates of Σ the values 1, 0) deduce a transformation of modulus $1+i$ by which f passes into $(1+i)\,\phi$; *i. e.*, ϕ is equivalent to one of the forms obtained by the preceding process. It only remains to show that when there are three of these forms, they constitute either one or three classes, but never two. For this purpose it is sufficient to consider the three semieven forms $\sigma_0=\left(1+i,\ 1,\ -\frac{D-1}{1+i}\right)$, σ_1, and σ_2, obtained by the preceding process from the form Σ. These forms satisfy the equations $\sigma_0\times\sigma_0=(1+i)\sigma_0$, $\sigma_1\times\sigma_1=(1+i)\sigma_2$, $\sigma_2\times\sigma_2=(1+i)\sigma_1$, $\sigma_1\times\sigma_2=(1+i)\sigma_0$; from which it follows that any one of the suppositions $\sigma_1=\sigma_2$, $\sigma_2=\sigma_0$, $\sigma_0=\sigma_1$ involves the other two.

* For the definition of the classes (σ_0), (σ_1), (σ_2) see the preceding note.

† The forms ϕ_0 and ϕ_1 are obtained by applying to f a complete set of transformations of modulus $1+i$, dividing the resulting forms by $1+i$, and retaining only those quotients which are uneven forms.

is one half of the number of uneven ambiguous classes, according as the classes (ϕ_0) and (ϕ_1) are identical or not; *i. e.*, according as the whole number of semieven classes is equal to or is one-half of the whole number of even classes.

The demonstration in the 'Disquisitiones Arithmeticæ,' that the number of genera of uneven forms of any determinant cannot exceed the number of uneven ambiguous classes of the same determinant, may be transferred without change to the complex theory. We thus obtain a proof (independent of the law of quadratic reciprocity and of the theorems which determine the quadratic characters of i and $1+i$) of the impossibility of one-half of the whole number of assignable generic characters; and from that impossibility, as we shall now show, the quadratic theorems are themselves deducible.

(1) If p is an uneven prime $\equiv 1$, mod 2, there are two genera of uneven forms of determinant p: of these one is the principal genus, and has the complete characters $\left(\frac{f}{p}\right)=1$, $\gamma=1$; the other, containing the form $(i, 0, +ip)$, has the particular character $\gamma=-1$; whence it follows that every uneven form of determinant p, which has the character $\gamma=+1$, is a form of the principal genus, and has the character $\left[\frac{f}{p}\right]=+1$. Again, if $p\equiv 1$, mod 4, the form $\left(2i, i, -\frac{p+1}{2i}\right)$ is an uneven form of determinant p; this form has the particular character $\gamma=-1$, because $-\frac{p+1}{2i}\equiv i$, mod 2; it is therefore not a form of the principal genus; but it has the character $\left(\frac{f}{p}\right)=1$, because $2i$ is a square; therefore, if $p\equiv 1$, mod 4, every uneven form of determinant p has the character $\left[\frac{f}{p}\right]=+1$.

(2) There is but one genus of forms of determinant i, and its complete character is $\alpha=+1$; there is also but one genus of forms of determinant $1+i$, and its complete character is $\beta=+1$.

(3) Let p and q be uneven primes of which the imaginary parts are even; to prove the law of reciprocity, it will suffice to show that if $\left[\frac{p}{q}\right]=1$, then $\left[\frac{q}{p}\right]=1$. The equation $\left[\frac{p}{q}\right]=1$ implies the existence of a congruence of the type $\omega^2-p\equiv 0$, mod q, and consequently of an uneven form of determinant p, and of the type $\left(q, \omega, \frac{\omega^2-p}{q}\right)$. This form has the character $\gamma=+1$, because $q\equiv 1$, mod 2; it therefore has the character $\left[\frac{f}{p}\right]=1$; *i. e.* $\left[\frac{}{p}\right]=1$.

(4) To prove the equation $\left[\frac{i}{p}\right]=(-1)^{\frac{1}{4}(Np-1)}$, in which we may sup-

pose that the uneven prime p is primary, it will suffice to show (i) that if $\left[\frac{i}{p}\right]=+1$, then $(-1)^{\frac{1}{4}(Np-1)}=1$; (ii) that if $(-1)^{\frac{1}{4}(Np-1)}=1$, then $\left[\frac{i}{p}\right]=1$. (i) Let $\left[\frac{i}{p}\right]=1$; then, if $\omega^2-i\equiv 0$, mod p, $\left(p, \omega, \frac{\omega^2-i}{p}\right)$ is a form of determinant i; it therefore has the character $\alpha=1$, *i. e.* $(-1)^{\frac{1}{4}(Np-1)}=1$. (ii) Let $(-1)^{\frac{1}{4}(Np-1)}=1$; then $p\equiv 1$, mod 4, and the form $(i, 0, ip)$ is an uneven form of determinant p; it therefore has the character $\left(\frac{f}{p}\right)=+1$; whence $\left[\frac{i}{p}\right]=+1$.

(5) Similarly, if $p=p_0+ip_1$ is an uneven and primary prime, to prove the equation $\left[\frac{1+i}{p}\right]=(-1)^{\frac{(p_0+p_1)^2-1}{8}}$ we shall show, (i) that if $\left[\frac{1+i}{p}\right]=1$, then $(-1)^{\frac{(p_0+p_1)^2-1}{8}}=1$; (ii) that if $(-1)^{\frac{(p_0+p_1)^2-1}{8}}=1$, then $\left[\frac{1+i}{p}\right]=1$. (i) Let $\left[\frac{1+i}{p}\right]=1$; then there is a form of determinant $1+i$ and of the type $\left(p, \omega, \frac{\omega^2-1-i}{p}\right)$; this form has the character $\beta=+1$; therefore $(-1)^{\frac{(p_0+p_1)^2-1}{8}}=+1$. (ii) Let $(-1)^{\frac{(p_0+p_1)^2-1}{8}}=+1$; then p is either $\equiv 1-2i$, or $\equiv 1$, mod $(1+i)^5$; if $p=(1+i)^5k+1-2i$, $([1+i]^3, i, 1-2ki)$ is an uneven form of determinant p; this form has the character $\gamma=+1$, and consequently it also has the character $\left[\frac{f}{p}\right]=+1$; therefore $\left[\frac{1+i}{p}\right]=\left[\frac{(1+i)^3}{p}\right]=+1$; if $p=(1+i)^5k+1$, one or other of the forms $([1+i]^5, 1, -k)$, and $([1+i]^5, 1+[1+i]^3, 1-k)$ is an uneven form of determinant p, having the character $\left[\frac{f}{p}\right]=1$; therefore in this case also $\left[\frac{1+i}{p}\right]=\left[\frac{(1+i)^5}{p}\right]=+1$.

IV. *The representation of Binary Forms of the principal Genus by Ternary Forms of Determinant* 1.

The solution of the general problem, "To find the representations (if any) of a given binary by a given ternary quadratic form," depends, in the case of complex as of real numbers, on the solution of the problem of equivalence for ternary forms. Extending the methods of Gauss to the complex theory, we find the necessary and sufficient condition for the primitive*

* If a matrix of the type $\left|\begin{matrix}\alpha, \beta\\ \alpha', \beta'\\ \alpha'', \beta''\end{matrix}\right|$ transforms a ternary into a binary quadratic form, the representation of the binary by the ternary form is said to be primitive when the three determinants of the matrix are relatively prime.

representation of a binary form f of determinant D by a ternary form of determinant 1 to be, that f should be a form of the principal genus; or, if $D \equiv \pm 1$, mod 4, that f should be a form either of the principal genus, or else of that genus which differs from the principal genus only in having the character $\gamma = -1$, instead of $\gamma = +1$. Again, because the reduction of Lagrange is applicable to complex binary forms, the reduction of Gauss* is applicable to complex ternary forms. It is thus found that the number of classes of such forms of a given determinant is finite; and in particular that every form of determinant 1 is equivalent to one or other of the forms $-x^2-y^2-z^2$ and $x^2+iy^2+iz^2$, of which the former cannot represent numbers $\equiv i$, or $\equiv 1+i$, mod 2; and the latter cannot primitively represent numbers $\equiv 2$, or $\equiv 2(1+i)$, mod 4. The method of reduction itself sup-

* If $F=ax^2+a'y^2+a''z^2+2byz+2b'xz+2b''xy$ is a ternary form of determinant Δ, and $Ax^2+A'y^2+A''z^2+2Byz+2B'xz+2B''xy$ its contravariant, by applying the reduction of Lagrange to the form $ax^2+2b''xy+a'y^2$, we can render $N.a \leqq 2\sqrt{N.A''}$ (Dirichlet in Crelle's Journal, vol. xxiv. p. 348); and by applying the same reduction to the form $A'y^2+2Byz+A''z^2$, we can render $N.A'' \leqq 2\sqrt{N.a\Delta}$. The reduction of Gauss consists in the alternate application of these two reductions until we arrive at a form in which we have simultaneously $N.a \leqq 2\sqrt{N.A''}$, $N.A'' \leqq 2\sqrt{N.a\Delta}$; and consequently $N.a \leqq 4\sqrt[3]{N.\Delta}$, $N.A'' \leqq 4\sqrt[3]{N.\Delta^2}$. If $\Delta=1$, we have $N.a \leqq 4$, $N.A'' \leqq 4$; whence a and A'' can only have the values $0, \pm 1, \pm i, \pm(1+i), \pm(1-i), \pm 2, \pm 2i$; and it will be found, on an examination of the different cases that can arise, that the reduction can always be continued until a and A'' are either both units, or both zero. In the former case, by applying a further transformation of the type

$$\begin{vmatrix} 1, & \mu'', & \mu' \\ 0, & 1, & \mu \\ 0, & 0, & 1 \end{vmatrix},$$

the coefficients b, b', b'' may be made to disappear; and we obtain a form equivalent to F, and of the type $\epsilon x^2+\epsilon' y^2+\epsilon'' z^2$, ϵ, ϵ', ϵ'' representing units of which the product is -1. In the latter case the form obtained by applying the reduction of Gauss is of the type

$$a'y^2+a''z^2+2byz+2b'xz;$$

whence $a'b'^2=1$, so that b' is a unit which we shall call ϵ; and the form $\epsilon^2 y^2 + a''z^2+2byz+2\epsilon xy$, by a transformation of the type

$$\begin{vmatrix} 1, & 0, & \mu' \\ 0, & 1, & \mu \\ 0, & 0, & 1 \end{vmatrix},$$

is changed into one of the four forms $\epsilon^2y^2+2\epsilon xz$, $\epsilon^2y^2+z^2+2\epsilon xz$, $\epsilon^2y^2+iz^2+2\epsilon xz$, $\epsilon^2y^2+(1+i)z^2+2\epsilon xz$; of which the first two by the transformations

$$\begin{vmatrix} \epsilon^{-1}i, & 0, & \epsilon^{-1} \\ \epsilon i, & \epsilon i, & \epsilon \\ 0, & -i, & -1 \end{vmatrix}, \quad \begin{vmatrix} 0, & 0, & -\epsilon \\ \epsilon^{-1}i, & 0, & 0 \\ 0, & i, & \epsilon^2 \end{vmatrix}$$

are changed into the form $-x^2-y^2-z^2$; the last two by the transformations

$$\begin{vmatrix} 0, & -\epsilon, & 0 \\ -\epsilon^{-1}, & 0, & 0 \\ 0, & -i\epsilon^2, & -1 \end{vmatrix}, \quad \begin{vmatrix} \epsilon^{-1}, & \epsilon^{-1}, & \epsilon^{-1}(1-i) \\ -\epsilon, & -\epsilon, & \epsilon i \\ 0, & -1, & i \end{vmatrix}$$

are changed into $x^2+iy^2+iz^2$. (See Disq. Arith. art. 272–274.)

plies a transformation of any given form of determinant 1 into one or other of those two forms.

If $D \equiv i$, or $1+i$, mod 2, no binary form of determinant D can be represented by $-x^2-y^2-z^2$, because D cannot be represented by the contravariant of that form, *i. e.* by the form $-x^2-y^2-z^2$ itself. Consequently, if $D \equiv i$, or $1+i$, mod 2, the binary forms of its principal genus are certainly capable of primitive representation by $x^2+iy^2+iz^2$.

If $D \equiv 1$, mod 2, no form of the principal genus can be primitively represented by $x^2+iy^2+iz^2$. Let $f=(a, b, c)$ be such a form, and let us suppose, as we may do, that b is even, so that $ac \equiv 1$, mod 2, and $a \equiv c \equiv 1$, mod 2 (the supposition $a \equiv c \equiv i$ is admissible, because f is of the principal genus); if possible, let the prime matrix

$$\left|\begin{matrix} \alpha\ , & \beta \\ \alpha',\ & \beta' \\ \alpha'',\ & \beta'' \end{matrix}\right|$$

(of which A, B, C are the determinants) transform $x^2+iy^2+iz^2$ into f; we have the equations $a=\alpha^2+i\alpha'^2+i\alpha''^2$, $c=\beta^2+i\beta'^2+i\beta''^2$, $D=A^2-iB^2-iC^2$, from which, and from the congruences $D \equiv a \equiv c \equiv 1$, mod 2, we infer the incompatible conditions $\alpha'+i\alpha'' \equiv \beta'+i\beta'' \equiv 0$, mod $1+i$, $A \equiv 1$, mod $1+i$; i. e. f is incapable of primitive representation by $x^2+iy^2+iz^2$. If, therefore, $D \equiv 1$, mod 2, the forms of its principal genus are capable of primitive representation by $-x^2-y^2-z^2$. We may add that when $D \equiv \pm 1$, mod 4, the forms of that genus which differs from the principal genus only in having the character $\gamma=-1$, instead of $\gamma=+1$, are capable of primitive representation by $x^2+iy^2+iz^2$, but not by $-x^2-y^2-z^2$.

Lastly, let $D \equiv 0$, mod 2. If $D \equiv 2$, or $\equiv 2(1+i)$, mod 4, D cannot be primitively represented by $x^2-iy^2-iz^2$, the contravariant of $x^2+iy^2+iz^2$; i.e. no form of determinant D can be primitively represented by $x^2+iy^2+iz^2$; so that forms of the principal genus are certainly capable of primitive representation by $-x^2-y^2-z^2$. But if $D \equiv 2i$, or $\equiv 0$, mod 4, the forms of the principal genus are capable of primitive representation by both the ternary forms $-x^2-y^2-z^2$ and $x^2+iy^2+iz^2$. For if $f=(a, b, c)$ be a form of the principal genus of any even determinant, f can only represent numbers $\equiv 0$, or $\equiv 1$, mod 2; so that a ternary form of determinant 1 and of the type

$$f+p''z^2+2qyz+2q'xz$$

will be equivalent to $-x^2-y^2-z^2$, or to $x^2+iy^2+iz^2$, according as $p'' \equiv 0$, or $\equiv 1$, mod 2, on the one hand, or $p'' \equiv i$, or $\equiv 1+i$, on the other hand. Again, if (k, k') is a value of the expression $\sqrt{(a, -b, c)}$, mod D, (in which we now suppose a uneven and b semieven or even), $\left(k+\frac{D}{1+i}, k'\right)$ is another value of the same expression; and it can be shown* that when

* If $f+p''z^2+2qy^2+2q'xz$ is a ternary form of det. 1, derived from the value (k, k') of the expression $\sqrt{(a, -b, c)}$, mod D, k is the coefficient of yz in the contravariant form. Hence $a=k^2-D(q'^2-ap'')$, or $ap''=q'^2+\frac{a-k^2}{D}$. Observing that $a \equiv 1$, mod 2

$D \equiv 2i$, or 0, mod 4, one of the two forms of determinant 1, and of the type

$$f+p''z^2+2qyz+2q'xz,$$

which are deducible by the method of Gauss from those two values, satisfies the condition $p'' \equiv 0$, or $\equiv 1$, mod 2, while the other satisfies the condition $p''=i$, or $1+i$, mod 2; that is, f is capable of primitive representation by both the forms $-x^2-y^2-z^2$ and $x^2+iy^2+iz^2$.

The preceding theory supplies a solution of the problem, "Given a form of the principal genus of forms of determinant D, to investigate a form from the duplication of which it arises." Let $f=(a, b, c)$ be the given form, and let us suppose (as we may do) that a and c are uneven. When $D \equiv i$, or $1+i$, mod 2, let

$$\begin{vmatrix} \alpha, & \beta \\ \alpha', & \beta' \\ \alpha'', & \beta'' \end{vmatrix}$$

be a prime matrix (of which the determinants are A, B, C) transforming $x^2+iy^2+iz^2$ into $(a, -b, c)$; and let ϕ represent the binary form $(C-iB, A, iC-B)$; then the matrix

$$\begin{pmatrix} \beta'+i\beta'', & \beta, & \beta, & -i(\beta'-i\beta'') \\ \alpha'+i\alpha'', & \alpha, & \alpha, & -i(\alpha'-i\alpha'') \end{pmatrix} \quad \ldots\ldots \quad (Z)$$

transforms f into $\phi \times \phi^*$; and is a prime matrix, for its determinants $C-iB$, $2A$, and $iC-B$ are not simultaneously divisible by any uneven prime (because A, B, and C are relatively prime), and are not simul-

---

$q'^2 \equiv 0$, or 1, mod 2, we see that $p'' \equiv 0, 1$, or $\equiv i, 1+i$, mod 2, according as $\frac{a-k^2}{D} \equiv 0, 1$, or $\equiv i, 1+i$, mod 2. But $\frac{a-k^2}{D} - \frac{a-\left(k+\frac{D}{1+i}\right)^2}{D} = (1-i)k+\frac{D}{2i}$; which is congruous to $1+i$, mod 2, if $D \equiv 0$, mod. 4, and to i, mod 2, if $D \equiv 2i$, mod 4, since k is evidently uneven in either case. From this it appears that if $\frac{a-k^2}{D} \equiv 0, 1$, mod 2, then $\frac{a-\left(k+\frac{D}{1+i}\right)^2}{D} = i, 1+i$, mod 2; that is, in one of the two forms $f+p''z^2+2qyz+2q'xz$, $p'' \equiv 0$, or 1, mod 2, and in the other $p'' \equiv i$, or $1+i$, mod 2.

* This assertion may be verified by means of the identity

$$\begin{aligned} &(q_1q_2-q_0q_3)(p_0xx'+p_1xy'+p_2x'y+p_3x'y')^2 \\ &+(q_0p_3+p_0q_3-q_1p_2-p_1q_2)(p_0xx'+p_1xy'+p_2x'y+p_3x'y') \\ &\qquad \times(q_0xx'+q_1xy'+q_2x'y+q_3x'y') \\ &+(p_1p_2-p_0p_3)(q_0xx'+q_1xy'+q_2x'y+q_3x'y')^2 \\ &=[(p_0q_2-p_2q_0)x'^2+(p_0q_3-p_3q_0+p_1q_2-p_2q_1)x'y'+(p_1q_3-p_3q_1)y'^2] \\ &\times[(p_0q_1-p_1q_0)x^2+(p_0q_3-p_3q_0+p_2q_1-p_1q_2)xy+(p_2q_3-p_3q_2)y^2]; \end{aligned}$$

in which we have to replace the quantities

$$\begin{matrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{matrix}$$

by the elements of the matrix (Z).

taneously divisible by $1+i$, because (Z) is congruous, for the modulus $1+i$, to the first or second of the matrices

$$\begin{pmatrix} 0, & 1, & 1, & 0 \\ 1, & 0, & 0, & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1, & 0, & 0, & 1 \\ 0, & 1, & 1, & 0 \end{pmatrix}, \quad \ldots\ldots \quad (Z')$$

according as $a \equiv i$, $c \equiv 1$, or $a \equiv 1$, $c \equiv i$, mod 2. Consequently ϕ is a form the duplication of which produces f. When $D \equiv 1$, or $\equiv 0$, mod 2, let the prime matrix

$$\begin{vmatrix} \alpha\ , & \beta \\ \alpha', & \beta' \\ \alpha'', & \beta'' \end{vmatrix}$$

transform $-x^2-y^2-z^2$ into $(a, -b, c)$. As we cannot have simultaneously $\alpha \equiv \beta$, $\alpha' \equiv \beta'$, $\alpha'' \equiv \beta''$, mod $(1+i)$, we may suppose that α and β are incongruous, mod $(1+i)$. If $\phi = (B+iC, iA, B-iC)$, the matrix

$$\begin{pmatrix} \beta'+i\beta'', & i\beta, & i\beta, & \beta'-i\beta'' \\ \alpha'+i\alpha'', & i\alpha, & i\alpha, & \alpha'-i\alpha'' \end{pmatrix} \quad \ldots\ldots \quad (Z)$$

transforms f into $\phi \times \phi$, and is a prime matrix, being congruous to one or other of the matrices (Z') for the modulus $1+i$, in consequence of the two suppositions that a and c are uneven, and that α and β are incongruous, mod $(1+i)$: so that f arises from the duplication of ϕ.

From the resolubility of this problem we can infer (precisely as Gauss has done in the real theory) that that half of the assignable generic characters which is not impossible corresponds to actually existing genera. We can also deduce a demonstration of the theorem that any form of determinant D can be transformed into any other form of the same genus, by a transformation of which the coefficients are rational fractions having denominators prime to 2D. For every form which arises from the duplication of an uneven primitive form—that is, every form of the principal genus—represents square numbers prime to 2D, and is therefore equivalent to a form of the type $\left(\lambda^2, \mu, \frac{\mu^2-D}{\lambda^2}\right)$. But $(1, 0, -D)$ is transformed into $\left(\lambda^2, \mu, \frac{\mu^2-D}{\lambda^2}\right)$ by $\begin{pmatrix} \lambda, & \frac{\mu}{\lambda} \\ 0, & \frac{1}{\lambda} \end{pmatrix}$; i. e. any two forms of the principal genus can be transformed into one another by transformations of the kind indicated. Again, if f_1, f_2 be two forms of any other genus, a form ϕ of the principal genus exists satisfying the equation $f_2 = \phi \times f_1$. But since ϕ can be transformed into the principal form, we can assign to the indeterminates of ϕ rational values, having denominators prime to 2D, which shall cause ϕ to acquire the value $+1$; and thus, from the transformation of f_2 into $f_1 \times \phi$, we deduce a rational transformation of f_2 into f_1, the coefficients of which have denominators prime to 2D. The truth of the converse proposition, "Two forms which are transformable into one another by rational transformations having denominators prime to 2D belong to the same genus,"

is evident from the definition of the generic characters themselves. The proposition itself is of some importance, as it furnishes a verification of the completeness of the enumeration of generic characters contained in Table III.

II. "Inquiries into the National Dietary." By Dr. E. Smith, F.R.S. Received April 28, 1864.

(Abstract.)

The paper contains an abstract of the scientific results of an inquiry which the author had undertaken for the Government into the exact dietary of large classes of the community, viz. agricultural labourers, cotton operatives, silk-weavers, needlewomen, shoemakers, stocking-weavers, and kid-glovers. The inquiry in reference to the first class was extended to every county in England, to North and South Wales and Anglesea, to the West and North of Ireland, and to the West, North, and part of the South of Scotland, whilst in reference to the other classes it was prosecuted in the towns where they were congregated.

The object of the investigation was to ascertain in the most careful manner the kind and quantity of food which constitutes the ordinary dietary of those populations; and the inquiry was in all cases made at the homes of the operatives.

The number of families included in the inquiry was 691, containing 3016 persons then living and taking food at home. The calculations of the nutritive elements are made upon the basis of an adult, two persons under the age of 10 and one over that age being regarded as an adult, and of the elements, the carbon and nitrogen are calculated in each article of food, whilst the free hydrogen is separately estimated as carbon upon the total quantities.

The author then cites the estimations which in his papers in the Philosophical Transactions for 1859 and 1861 he had made of the quantity of carbon and nitrogen emitted by the body under various conditions, and computes on those bases the amounts of those substances which are required as food by various classes of the community. He then proceeds to state the quantities which have been actually found in the dietaries of the persons included in this investigation, and the great variations which the inquiry had brought to light. He also compares the nutriment with the cost of it in the food, and states the proportion which the nitrogen bears to the carbon in each of the classes and in the different localities.

Each article of food is then considered separately, and the frequency with which, as well as the average quantity in which, it was obtained by these populations is stated.